CST8230 – IT Security Basics

Corrector

Mid-Term Exam

Date: March 1st, 2012
45 minutes

Exam is out of 45 Marks

Professor: Patrick Ouellette

All the usual disclaimers and provisions apply;
***you know the drill*.**

If an explanation isn't listed beside the answer, then the answer comes directly from the course content slides.

Name: _____

Student #: _____

Signed: _____

Instructions

1) Write your name on the SCANTRON sheet & the exam front page.

2) CALCULATORS ARE NOT PERMITTED.
   Only cheat-sheet allowed is the included SANS TCP/IP guide
   (*back of the exam*)

3) All questions in ***Section A*** are to be answered in the SCANTRON.
   - **35** Multiple Choice questions in ***Section A***, worth *1 mark each.*
   - Write on the SCANTRON sheet using a pencil.
     ERASE completely to change your answer.
   - The answer to question **21** is **B**.
   - Double-check to ensure you have correctly coded all your answers on the SCANTRON sheet BEFORE time runs out.
     I will not check the exam for answers.

4) The question in ***Section B*** will marked directly from the exam.
   - **5** short answer questions in ***Section B***, worth *2 marks each.*

5) You have ***45 minutes*** to complete this test.

6) This mid-term is worth ***20% of your final grade***.

Section A – Multiple Choice Questions

1. Based on the highlighted portion of the captured packet below, what **protocol** is being carried as payload within this IP packet?

4500 0064 0000 4000 40***11*** b755 c0a8 0101

A - IP
B - UDP (*0x11 -> 17 thus UDP*)
C - TCP
D - ICMP
E - None of the above

2. The ICMP protocol is specifically designed to:

A- Check & report on network error conditions
B- Generate networking stats
C- Control traffic flow across networks
D- Track end-to-end connectivity
E- None of the above

3. It is possible to capture packets from the network that are not destined for your machine.

A - False
B - True (*that[s what promiscuous mode is for!*)

4. In security environments, ***Authorization*** means

A - Confirming your identity with an element unique to the person
B - Supplying your identity
C - Using your confirmed identity to assign access rights
D - Tracking what users are doing while accessing the systems
E - None of the above

5. During a packet capture, you notice a couple of TCP packets with the "**F**" flag and some "**A**" flags. What is ***most likely*** going on?

A- A TCP/IP session setup process
B- An ICMP Request / Reply process
C- An ARP process
D- A UDP-based FTP session
E- A TCP/IP session shutdown process

6. The loss or omission of any one of the security goals is known as:

A- A risk
B- A compromise
C- A hole
D- A fault
E- A vulnerability

7. If you run password crackers or packet sniffers at work, which of the following is true?

A-	You must encrypt or destroy cracked passwords
B-	E-mail any users using inappropriate software on the network to inform them you know
C-	Don't crack passwords that meet the company's password policy
D-	You must have permission from management before proceeding
E-	All of the above

8. Packet sniffing is considered to be a form of:

A-	Passive reconnaissance
B-	Active reconnaissance
C-	Countermeasure
D-	Denial of Service
E-	Preliminary reconnaissance

9. The ***Data*** _____ is the person having responsibility and authority for data, while the ***Data*** ___ is the entity temporarily accessing and/or modifying the data.

A-	Custodian, Owner
B-	Owner, Manager
C-	Owner, Custodian
D-	Manager, Custodian
E-	Administrator, Manager

10. Based on the highlighted portion of packet code below, what protocol is being used?
4500 0064 0000 4000 4001 b755 c0a8 0101

A -	TCP
B -	ICMP
C -	UDP
D -	ARP
E -	None of the above (***indicates IPv4 and 20 byte header***)

11. Which of the following statements about ***session hijacking*** is false?

A-	Most computers are vulnerable to this form of attack
B-	Hijacking is preventable
C-	Hijacking is very dangerous (*this ain't hijacking a plane…*)
D-	Hijacking is quite simple with the proper tools at hand
E-	It is very hard to detect that hijacking has taken place

12. Which of the following is an example of e-mail phishing?

A-	An e-mail about products for "male insufficiency" (*spam*)
B-	A link to a site about "free" phones (*spam*)
C-	When someone uses your e-mail address when sending out spam (*hacking*)
D-	An e-mail from your provider asking for you to confirm you password back in e-mail
E-	None of the above

13. The term ***No-Tech Hacking*** refers to:

A-	The hacker's ability to make the attack process look easy
B-	A way for non-technically oriented people to learn how to hack
C-	Methods used by a hacker to obtain information without the use of technology
D-	A hack that's so simple can be done without using a lot of technology
E-	None of the above

14. When using a packet sniffer, such as TCPDump, what parts of the packet can you examine through the software?

A -	IP header content
B -	Protocol header (TCP, UDP, ICMP, etc) content
C -	Payload
D -	A and B only
E -	A, B & C

15. Which of the following is not one of the Security Goals?

A-	Security
B-	Accountability (*part of the security functions, not goals*)
C-	Ease of Use
D-	Functionality
E-	They are all Security Goals

16. Your system receives a few packets, but no connection seems to be established. When you look at the logs, you notice you received a few SYN packets, immediately followed by RST packets, but no ACK packets. What's could be happening?

A-	SYN Stealth Open Port scan from Nmap
B-	XMAS Open Port scan from Nmap
C-	Hacker trying to identify the service running on a port
D-	TCP/IP stack has failed
E-	None of the above

17. Security policies should be written while keeping in mind the protection of:
(***Select all that apply***)

A-	Information
B-	People
C-	Bandwidth
D-	Assets
E-	Connectivity

18. Which of the following is considered typical reasons why hackers attack systems?

A -	Profit
B -	Religious / political / ethical reasons
C -	"Mount Everest" syndrome
D -	Revenge
E -	All of the above

19. In the ***CIA Triad***, _____ is responsible for ensuring that legitimate users maintain access to information and resources they need access to.

A -	Accountability
B -	Authentication
C -	Integrity
D -	Confidentiality
E -	Availability

20. In terms of security, ***Social Engineering*** is considered to be a form of:

A-	Cracking
B-	Illegal information warfare activity
C-	Non-Technical hacking
D-	Technical hacking
E-	All of the above

21. A ___ attaches itself to a program or file so it can spread from one computer to another with the file as it travels, leaving infections as it travels.

A-	Worm
B-	Virus
C-	Trojan
D-	Rootkit
E-	None of the above

22. How did **Vince**, the Physical Security Expert mentioned in the "***No Tech Hacking***" movie, manage to enter the secure building ... *What specifically did he do and what did he use to do it*?

A-	Watched smokers for in/out patterns
B-	Used a wet washcloth and a coat-hanger to trigger the fire-door contact bar after hours
C-	He broke in through a window
D-	He took pictures of corporate badges, created a fake and used it to enter the building
E-	None of the above

23. A typical ***Man-in-the-Middle attack*** attempts to exploit a ___ between computers.

A-	Session captures
B-	Connection control flags
C-	UDP packets
D-	TCP/IP shutdown session
E-	Trust relationship

24. In security environments, ***Authentication*** refers to:

A -	Confirming your identify with an element unique to the individual
B -	Supplying your identity
C -	Using your identity to assign access rights
D -	Tracking what users are doing while accessing the systems
E -	None of the above

25. The TCP three-way handshake used to **open** a TCP connection uses 3 packets. What 2 flags are required to be set across these 3 packets? (***Select all that apply***)

A -	SYN Flag
B -	Payload Flag
C -	FIN Flag
D -	ACK Flag
E -	RST Flag

26. Which one of the tools below can be used as an effective **vulnerability** scanner?

A -	Nmap (*port scanner only*)
B -	Snort (*IDS*)
C -	Nessus
D -	Nmap (*port scanner only*)
E -	Tcpdump (*sniffer only*)

27. A closed port will respond to a ***SYN*** Packet with a(n) ***RST*** packet

A-	True *(has to, as per RFP, since there's nothing to respond to the request)*
B-	False

28. ***Computer A w***ishes to open a TCP session with ***Computer B***. If ***Computer A***'s initial sequence number is 145678913, then ***Computer B*** will respond with:

A-	A randomly generated initial sequence number of its own and an acknowledgement number of **145678914 (***ISN+1***)**
B-	A randomly generated initial sequence number of its own and no acknowledgement number since no data was received
C-	Only an acknowledgment number of 145678914
D-	Only an acknowledgement number of 145678913
E-	A randomly generated initial sequence number of its own and a randomly generated acknowledgement number

29. From the perspective of ***Risk Management***, security can be defined as:

A-	Ensuring the company so that security incidents don't cost the organization a lot.
B-	Reducing / minimizing the risks to the organization and its assets to an acceptable level.
C-	Protecting the organization's assets
D-	All of the above
E-	None of the above

30. The loss of one of the goals of security through an incident is known as a:

A-	Hole
B-	Vulnerability
C-	Risk
D-	Compromise
E-	Threat

31. A fragmented IP datagram will only be reassembled by:

A-	The router closest to the destination
B-	Any router along the path when the MTU changes to permit a larger datagram
C-	By the host it is destined for (*as per RFP*)
D-	By the application processing the information datagram
E-	None of the above

32. ____ is designed as **a connectionless protocol**.

A-	IGRP
B-	TCP
C-	UDP
D-	FTP
E-	None of the above

33. Each TCP connection on a given system can be ***uniquely*** identified by:

A-	Source and Destination IP
B-	Source and Destination port
C-	Sequence Number
D-	Connection Number
E-	A & B only (*i.e. Socket*)

34. ___ spread from computer to computer, but unlike other malware, it has the ability to travel and replicate itself without any user intervention.

A-	Worm
B-	Trojan
C-	Virus
D-	Rootkit
E-	None of the above

35. Which one of the following is NOT a fundamental principle of the Computer Security Triad?

A -	Confidentiality
B -	Ease of Use
C -	Availability
D -	Integrity
E -	Accountability

Section B – Short Answers

1. Explain the difference between **Threat** and **Vulnerability**.

Threat:

- *something that could cause a security issue if allowed to get in (e.g. virus, hacker, etc)*
- *doesn't have any "Teeth" without a vector/vulnerability to allow it to manifest*
- *external to system*

Vulnerability:

- *a potential security hole that may exist on the system and needs to be shored up/protected against or patched to ensure it isn't exploited by a threat*
- *So long as it exists, the risk of exploit/compromise exists*
- *Internal to system*

Risk = Vulnerability x Threat

2. Define the term and process of "***active reconnaissance***" & give some examples.

The goal is ***to gather more direct information while remaining unseen***, looking to improve the quality and depth of *passive recon* information unearthed while still threading lightly (*without setting off too many security alarms*).

Visibility becomes a possibility at this level (*not as covert***),** since it is done using methods & tools that might potentially trigger security responses**, *but the intent remains to be as unobtrusive and invisible as possible***.

Attackers will looks for information on:

- *Hosts that are accessible*
- *Known trust relationships*
- *Locations of and specific details about routers and firewalls*
- *Operating systems & Rev/SP in use*
- *Ports that are open/filtered*
- *Services that are active/running*
- *Versions of applications/services accessible on ports*
- *Etc…*

Examples include: ***Probing and scanning to find vulnerabilities; searching for non-public, protected or privileged information; system profiling; war dialing/driving; hacking; social engineering the target; etc***

3. Define and explain the concept of **Least Privileges**?

Every security object (*user, process, resource, etc***) should only be assigned the minimum permissions/access *required* to be able to accomplish its assigned task(s), no more.**

4. What are the 3 main types/areas of security, excluding Safety?
   Give a bit of detail to explain each one.

   A. System Security
   i) Protection of information, capabilities and services on a system/server
   (1) SANs, servers, desktops, network devices, etc…
   B. Communication Security
   i) Protection of information while it's being transmitted
   (1) Also includes protection of the medium itself (in so far as it's possible)
   C. Physical Security
   i) Protection from physical access to computer, communications equipment, facilities and personnel from damage or theft
   (1) *All logical security controls must include physical security*

5. Explain why ***physical security*** is a necessary and integral part of IT/IS Security.

   Without proper physical security, you can't protect systems from direct access, theft and/or physical damage. *If the enemy has direct access to the hardware/information, they can take their time, use a much broader set of skills & tools to breach any security AND do it at their leisure.*

   Then there's the "building access" issue, which could leads to above. *Even if they can't get to the hardware or info, having access means they might be able to gain insider knowledge of how the company operates and gain invaluable information for escalating access.*

   Add industrial spying and associated abilities*, and any direct line of sigh access can be considered a major security risk/breach.*